ADVISEN
Insurance Intelligence

INFORMATION SECURITY & CYBER LIABILITY RISK MANAGEMENT:

October 2012

Sponsored by:

ZURICH

INFORMATION SECURITY & CYBER LIABILITY RISK MANAGEMENT:

The Second Annual Survey on the Current State of and Trends in Information Security and Cyber Liability Risk Management

Executive Summary

As awareness grows due to media coverage of high profile data breaches, pending cyber legislation and continued advisories from cyber security professionals, information security and other cyber risks continue to represent at least a moderate threat to a majority of risk professionals. Board Members and Executive Management increasingly are recognizing the risks of a wide range of exposures such as lost or stolen data, violation of privacy laws, intellectual property infringement, social media, mobile devices, BYOD (Bring Your Own Device) and cloud computing. Although the strategies for addressing these risks vary, more and more organizations are adopting an enterprise-wide – or at least a multi departmental – approach to information security and cyber liability risk management. Insurance also is increasingly becoming a part of more organizations cyber risk management strategy.

Board Members and Executive Management increasingly are recognizing the risks of a wide range of exposures such as lost or stolen data, violation of privacy laws, intellectual property infringement, social media, mobile devices, BYOD (Bring Your Own Device) and cloud computing.

About The Survey and the Respondents

For the second consecutive year Advisen Ltd has administered a survey sponsored by Zurich to gain insight into the current state of and ongoing trends in information security and cyber liability risk management. The survey was conducted for three weeks, beginning September 10, 2012 and ending October 1, 2012. Invitations to participate were distributed by email to 8,248 risk managers, insurance buyers and other risk professionals. The survey was completed at least in part by 511 respondents, for a response rate of 6 percent.

The largest percentage of respondents (49.0 percent) classified themselves as members of risk management departments (not head), followed closely by Chief Risk Manager/Head of Risk Management Department at 48.0 percent. Respondents with more than 20 years of risk management and insurance experience represented the largest group at 44.4 percent of the

The vast majority of respondents (86.7 percent) believe that cyber and information security risks pose at least a moderate threat to their organization.

total, followed by 28.0 percent with between 11-20 years, 16.2 percent between 6-10 years and 10.6 with 5 years or less.

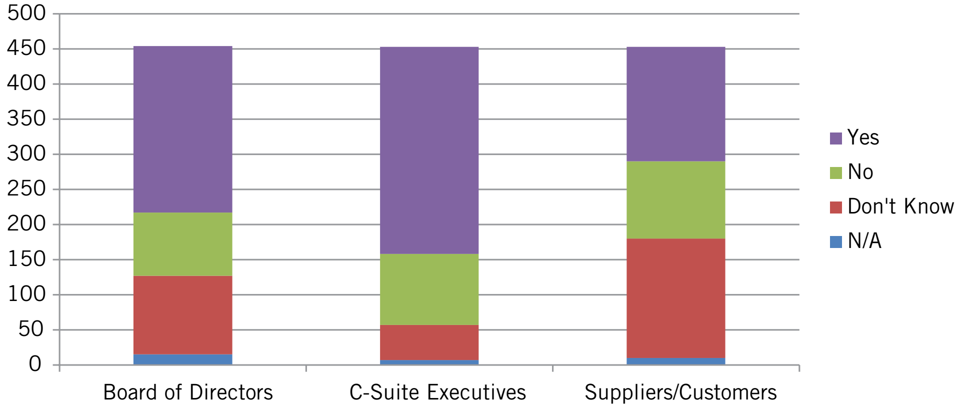
Businesses from an array of industries are represented. Segmented by 13 macro segments, Government and Nonprofit accounts for the largest industry sector with 15.3 percent of the total respondents, followed by Healthcare at 13.0 percent, Industrials at 12.4 percent, Consumer Discretionary at 8.8 percent, Professional Services at 8.6 percent, Utilities at 6.9 percent, Consumer Staples at 6.5 percent, Nonbank Financial at 5.9 percent, Banks at 5.5 percent, Education at 5.3 percent, Materials at 4.5 percent and Energy and Telecommunications both at 3.7 percent respectively. The survey also has a wide representation of companies based on size but is slighted weighted towards larger companies with 61.3 percent of respondent companies having revenues in excess of $1 billion.

Perception of Cyber Risks

The vast majority of respondents (86.7 percent) believe that cyber and information security risks pose at least a moderate threat to their organization. This is nearly identical to the 2011 response at 86.0 percent. However, while the perception of risk is basically unchanged for risk management and insurance professionals, it is noticeably higher for Board Members and C-Suite Executives. In response to the question "In your experience, are cyber risks viewed as a significant threat to your organization by:" 52.2 percent said "yes" for Board of Directors and 65.1 percent said "yes" for C-Suite Executives. Compared with the 2011 survey, this is an increase of 7.1 points for both the Board of Directors and C-Suite Executives. (Exhibit 1)

EXHIBIT 1

In your experience, are cyber risks viewed as a signifcant threat to your organizaton by:



Sponsored by: ZURICH

On a scale of one to five, with 5 as very high risk and 1 as very low risk, "privacy violation/data breach of customer records" was the biggest concern of respondents, with 63.6 giving it a rating of 4 or 5.

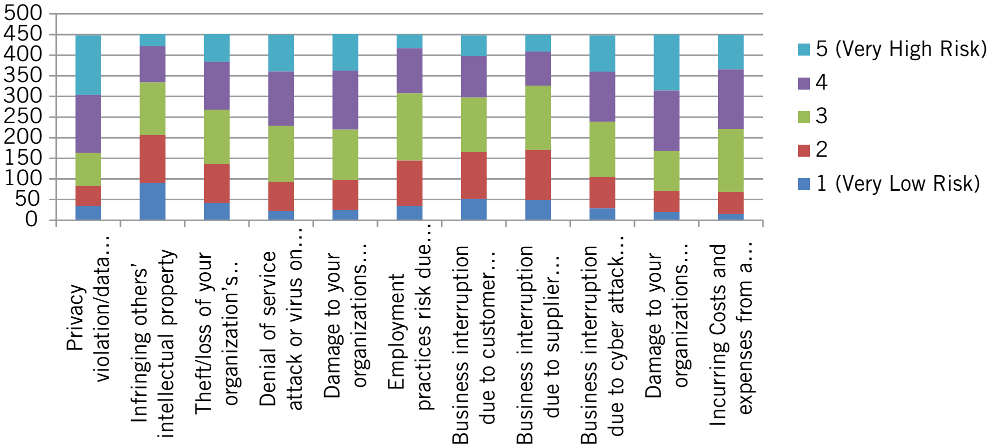
In 2012, much has been discussed regarding the increase in cyber-crimes targeting small and mid-size businesses. In response to the question "How would you rate the potential dangers posed to your organization by cyber & information security risks?" the smallest companies (revenues less than $250 million) still viewed cyber risks less seriously than their largest counterparts (revenue greater than $10 billion), with 81.8 percent of smaller companies saying the risks pose at least a moderate danger compared to 95.9 percent of large companies. The percent difference, however, is shrinking. In 2011, there was a 17.9 point difference between the percentage of the smallest and largest companies, while in 2012 there is only 14.1 point difference.

On a scale of one to five, with 5 as very high risk and 1 as very low risk, "privacy violation/data breach of customer records" was the biggest concern of respondents, with 63.6 giving it a rating of 4 or 5. This was followed closely by "damage to your organizations reputation resulting from a data breach" with 62.7 percent and "damage to your organizations reputation via social media" with 52.1 percent.

In contrast, the exposures that were perceived as representing the lowest risks, and had the highest percentage of respondents providing a rating of a 1 or 2, included "infringing on others' intellectual property" with 45.7 percent, "business interruption due to supplier cyber disruptions" with 37.8 percent and "business interruption due to customer cyber disruptions" at 36.8 percent. (Exhibit 2)

EXHIBIT 2

From the perspective of your organization, please rank the following on a scale of 1 to 5, with 5 as a very high risk and 1 as a very low risk.



More organizations are beginning to believe that it is the responsibility of the entire organization to mitigate risks.

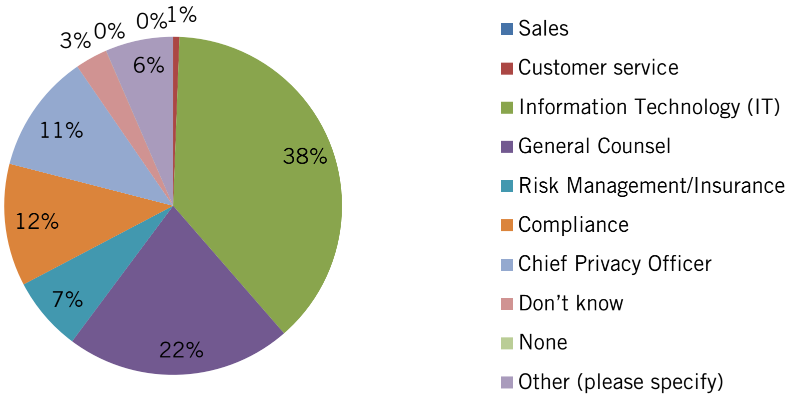
Disaster Response

Research has shown that organizations with a comprehensive disaster response plan in place before a breach occurs fare much better after a major breach than those that do not. According to the results of this survey, it appears that this message is indeed being received. Of the total respondents, 80.4 percent said that they have a disaster response plan in place. This represents a 12.4 point increase from 2011.

In response to the question "In the event of a data breach, which department in your organization is PRIMARILY responsible for assuring compliance with all applicable federal, state or local privacy laws including state breach notification laws?" consistent with the 2011 survey, the most respondents answered IT at 38.0 percent followed by General Counsel at 21.6 percent. (Exhibit 3)

EXHIBIT 3

In the event of a data breach, which department in your organization is PRIMARILY responsible for assuring compliance with all applicable federal, state, or local privacy laws including state breach notification laws?



Cloud computing is becoming a popular alternative for business seeking to take advantage of its cost effectiveness and increased storage capacity.

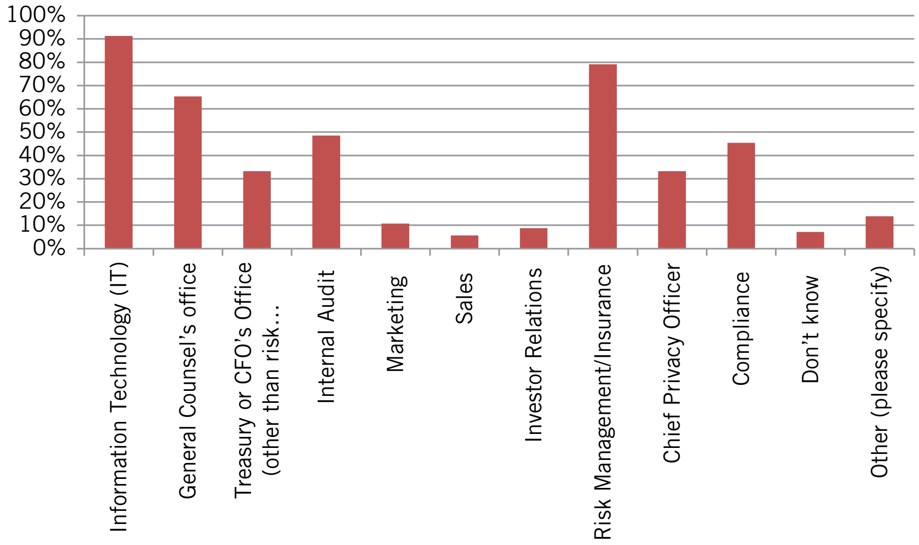
Information Security and Cyber Risk Management Focus

In response to the question "are information security risks a specific risk management focus within your organization?" 72.5 percent responded yes, 22.9 percent responded no. This was consistent with the 2011 survey where respondents were asked the same question and 71.6 percent said yes and 25.2 said no. Additionally, information security is a risk management focus of 71.0 percent of organizations with revenues less than $1 billion and 74 percent with revenue greater than $1 billion. However, for the organizations with revenues in excess of $10 billion it is a risk management focus for 83.8 percent.

More organizations are beginning to believe that it is the responsibility of the entire organization to mitigate risks. When asked "Does your organization have a multi-departmental information security risk management team or committee?" 61.4 percent said yes compared to 57.2 percent who said yes in 2011. The department or functions that are most likely to have representation in the information security risk management team are IT with 91.3 percent, Risk Management/Insurance 79.1 percent, General Counsel 65.3, Internal Audit 55 percent, Compliance 45.4 percent, Treasury or CFO 33.2 percent, Chief Privacy Officer 33.2 percent, Other 13.8 percent, Marketing 10.7 percent, Investor Relations 8.7 percent, Sales 5.6 percent. 7.1 percent did not know. (Exhibit 4)

EXHIBIT 4

Which departments are represented on your cyber risk management team or committee?

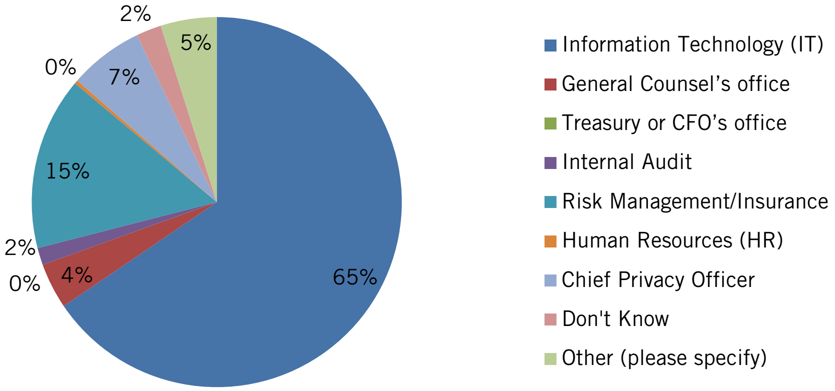


Although information security and cyber risks were widely acknowledged as serious concerns, cyber liability insurance is still purchased by less than half of the organizations.

While the IT department is still acknowledged as the front line defense against information losses and other cyber liability risks, the survey shows that a slow trend may be occurring and that responsibility is being shifted to the Risk Management/Insurance department. In response to the question "Which department is PRIMARILY responsible for spearheading the information security risk management effort?" 65.5 percent said it was the responsibility of the IT department compared to 73.2 percent in 2011, followed by 15.1 percent who said it was the Risk Management/Insurance department's responsibility compared to 13.2 percent in 2011. (Exhibit 5)

EXHIBIT 5

Which department is PRIMARILY responsible for spearheading the information security risk management effort?



Social media increasingly is being recognized as an exposure that requires risk management attention. As noted above, more than half of the respondents consider reputational damage via social media a significant threat to their organization. Of the companies surveyed, 78.7 percent have a written social media policy, a 15.1 point increase over 2011.

Mobile Devices and Cloud Computing

Included in this year's survey were questions on two of the biggest information security and cyber liability topics of 2012, mobile devices and cloud computing. Respondents were asked "Does your organization have a mobile device security policy?" 74.8 percent said yes, 14.6 percent said no and 10.6 percent did not know. Larger companies (those in excess of $1 Billion in revenue) are more likely to have a mobile device security policy with 84.9 percent responding yes, compared to only 61.8 percent of the smaller companies (those less than $1 Billion in revenue).

Respondents claiming to have a comprehensive crisis response plan in place shot up materially – from about two thirds in 2011 to four out of five respondents in 2012.

Businesses also are increasingly allowing their employees to use their personal mobile device for business purposes. As a result, these devices are now capable of accessing proprietary company information and creating a significantly more difficult exposure to control. When asked "Does your organization have a bring your own device (BYOD) policy?" 36.2 percent responded yes, 39.6 percent responded no, and 24.2 percent did not know. A more granular analysis of this question shows that large companies are more likely to have a BYOD policy with 45.0 percent of large companies responding yes compared to only 27.4 percent of smaller companies.

Cloud computing is becoming a popular alternative for business seeking to take advantage of its cost effectiveness and increased storage capacity. However, the idea of warehousing propriety business information on a third-party server has led many to question and/or trust its security. Respondents were asked "Does your organization use cloud computing services?" 44.7 percent said yes, 33.9 percent said no, and 21.4 percent did not know. Respondents were also asked "Is cloud computing part of your data security risk management process?" 38.7 percent said yes, 19.2 percent said no, and 27.6 did not know.

The Role of Insurance in Information Security and Cyber Risk Management

Although information security and cyber risks were widely acknowledged as serious concerns, cyber liability insurance is still purchased by less than half of the organizations. This percentage, however, is trending upward. Survey participants were asked "Does your company purchase cyber liability insurance?" 43.9 percent of respondents said yes compared to only 35.1 percent in 2011, and 49.9 percent said no compared to 60.1 percent in 2011. Brand restoration coverage is currently being purchased by 17.5 percent of the companies surveyed.

Of those who purchase coverage, 37.5 percent said that they have purchased coverage for less than two years, 42.2 percent said between three and five years and 20.3 percent said over 5 years. This suggest that the number of organizations that recognize the role that insurance can play as part of an information security and cyber risk management program continues to increase.

The percentage of companies considering purchasing cyber liability insurance in the next year remained consistent with 2011. Companies that currently do not purchase cyber liability insurance were asked "Are you considering buying this coverage in the next year?" 25.1 percent said yes, 48.7 percent said no and 26.2 percent do not know. These percentages continue to indicate that this coverage represents a growth opportunity for brokers and insurers.

Analysis and Conclusions

Two data points – the 2011 survey and the 2012 survey – provide an indication of how attitudes and practices are changing. Subsequent surveys will provide much stronger readings on trends in this important area. Based on these preliminary indications, however, it is clear that risk managers regard data security, privacy and reputation risks as at least a moderate threat, and it appears that the seriousness of the threat is increasingly recognized by strategic decision makers.

Although the vulnerabilities of small and mid-size business has received increased media attention in 2012, larger organizations continue to be more concerned with the risk as opposed to their smaller counterparts, and as a whole continue to be more involved in enterprise-wide risk management. While concerns about cyber-related risk varied somewhat by size of organization, this year's survey indicates overall greater attention to risk management and insurance issues. A higher percentage of respondents said their organizations have a multi-departmental team focused on data security and privacy as compared to last year. Respondents claiming to have a comprehensive crisis response plan in place shot up materially – from about two thirds in 2011 to four out of five respondents in 2012. The percentage of organizations purchasing cyber-related insurance coverages also was significantly higher, with nearly 44 percent of participating organizations purchasing insurance in 2012 as compared to about 35 percent in 2011.

Although the vulnerabilities of small and mid-size business has received increased media attention in 2012, larger organizations continue to be more concerned with the risk as opposed to their smaller counterparts, and as a whole continue to be more involved in enterprise-wide risk management.

Not surprisingly, IT departments continue to spearhead data security and privacy initiatives in most organizations. Risk managers, however, seemingly are playing increasingly significant roles in the process. The percentage of organizations where Risk Management/Insurance led the data security risk management program increased slightly to about 15 percent, as compared to about 13 percent in 2011. In nearly 80 percent of organizations with multi-departmental data security and privacy teams, the Risk Management/Insurance department is represented on the team.

One apparent deficiency in the data security risk management process of many organizations has to do with data breach reporting requirements. Presently, 46 states have data breach reporting laws, with requirements that can vary materially from state to state. As was the case with the 2011 survey, the vast majority of respondents said the IT department has principal responsibility for fulfilling breach notification requirements. However, IT departments at most companies are seemingly ill-equipped for this responsibility.

Presently, 46 states have data breach reporting laws, with requirements that can vary materially from state to state.

About Zurich

Zurich in North America is a part of Zurich Insurance Company (Zurich), an insurance-based financial services provider with a global network of subsidiaries and offices in North America and Europe as well as in Asia Pacific, Latin America and other markets. Founded in 1872, the Group is headquartered in Zurich, Switzerland and employs approximately 60,000 people serving customers in more than 180 countries, including more than 9,500 employees in North America.

Zurich entered the U.S. market in 1912. According to Highline Data LLC (NAIC 2008), Zurich in North America (www.zurichna.com) is the second-largest writer of commercial general liability insurance and the fourth-largest commercial property-casualty insurance company, serving the global corporate, large corporate, middle market, specialties and programs sectors. Zurich's risk engineering services in the United States are provided by Zurich Services Corporation. ■